UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE DE DIREITO

A PROTEÇÃO DE DADOS PESSOAIS E OS CONTRATOS DE SEGURO

MARIANA COELHO DE MENDONÇA

Rio de Janeiro

2017/1º SEMESTRE

MARIANA COELHO DE MENDONÇA

A PROTEÇÃO DE DADOS PESSOAIS E OS CONTRATOS DE SEGURO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob orientação do Professor Dr. Guilherme Magalhães Martins.

Rio de Janeiro

2017/1º SEMESTRE

FICHA CATALOGRÁFICA

CIP - Catalogação na Publicação

C539p

COELHO DE MENDONÇA, MARIANA
A PROTEÇÃO DE DADOS PESSOAIS E OS CONTRATOS DE SEGURO / MARIANA COELHO DE MENDONÇA. -- Rio de Janeiro, 2017.
51 f.

Orientador: GUILHERME MAGALHÃES MARTNS.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2017.

1. PRIVACIDADE. 2. TRATAMENTO DE DADOS. 3. DADOS PESSOAIS. 4. PROTEÇÃO DE DADOS . 5. CONTRATO DE SEGURO. I. MAGALHÃES MARTNS, GUILHERME, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

MARIANA COELHO DE MENDONÇA

A PROTEÇÃO DE DADOS PESSOAIS E OS CONTRATOS DE SEGURO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob orientação do Professor Dr. Guilherme Magalhães Martins.

Data de Aprovação: _____/_____/_____

Banca Examinadora:

_____

Orientador Professor Dr. Guilherme Magalhães Martins

_____

Membro da Banca

_____

Membro da Banca

Rio de Janeiro

2017/1º SEMESTRE

AGRADECIMENTOS

Agradeço primeiramente a Deus, que com sua infinita sabedoria me aponta os caminhos para vencer os obstáculos e dificuldades da vida.

À minha querida família e aos amigos que me acompanharam ao longo desta jornada.

À Cristiane da Silva Coelho de Mendonça, Roberto Rocha de Mendonça e Gabriel Coelho de Mendonça pelo amor incondicional, pela paciência, incentivo e apoio diário para a elaboração desse trabalho.

À toda equipe da CNseg pela contribuição na minha vida acadêmica e profissional.

À Faculdade Nacional de Direito da UFRJ pelos 05 (cinco) anos de aprendizado, pelas amizades e pelo sentimento do que é ser da Nacional.

Ao meu orientador Professor Guilherme Martins por dividir com brilhantismo seus conhecimentos comigo e pelo auxílio no presente estudo.

RESUMO

A discussão acerca do direito à privacidade, da proteção de dados pessoais e dos contratos de seguros. Na sociedade de informação se utilizam cada vez os dados pessoais como insumo para a atividade empresarial. Em especial, o setor de seguros é baseado na informação, na medida em que para a melhor precificação do risco do seguro se faz necessário à análise dos dados pessoais. Contudo, há situações em que tal análise pode ser discriminatória, sobretudo quanto a utilização de dados sensíveis. A solução encontrada na análise é o equilíbrio dos princípios, e o uso da informação a partir da informação ao consumidor quanto a finalidade do uso de dados e seu expresso consentimento. Por fim, abordou-se em linhas gerais a proposta de regulamentação brasileira sobre dados pessoais, já que diferente da maioria dos países, ainda não há no Brasil uma regulamentação sobre o tema.

Palavras-chave: Privacidade; Tratamento de Dados; Dados Pessoais; Proteção de Dados; Contrato de Seguro.

ABSTRACT

The discussion of the right to privacy, the protection of personal data and insurance contracts. In the information society they use personal data as inputs for business activity. In particular, the insurance sector is based on information, as far as the best insurance risk pricing is necessary to analyse personal data. However, there are situations where such analysis can be discriminatory, especially when using sensitive data. The solution found in the analysis is the equilibrium of the principles, and the use of information from the consumer information regarding the purpose of the use of data and its express consent. Finally, the proposal for a Brazilian regulation on personal data has been addressed in general, as different from most countries, there is still no regulation on the subject in Brazil.

Key words: privacy; Data processing; Personal data; Data protection; Insurance contract.

SUMÁRIO

1. INTRODUÇÃO

O presente estudo versa sobre a proteção de dados pessoais no contexto da sociedade atual, trará o desafio da sociedade digital para equilibrar o direito a privacidade, na versão da proteção de dados pessoais com o interesse comercial referente ao setor de seguros, sob a luz dos princípios da proteção de dados pessoais.

Se há séculos atrás a terra era o instrumento de poder, sendo substituída pelo ferro, madeira, carvão e petróleo atualmente, na era da sociedade de informação, o instrumento de poder é a informação.

A sociedade de informação não é uma sociedade de bens, mas de serviços em que a posse da informação prevalece sobre a posse dos bens de produção.

Com o avanço da tecnologia e a sofisticação da coleta, processamento e utilização de dados pessoais, a informação tornou-se grande matéria prima para a economia mundial, sendo insumo da produção de um modelo econômico voltado à individualização e especialização do produto.

Assim sendo, a intensificação do fluxo e do processamento de informações alterou a perspectiva clássica de privacidade relacionada ao isolamento e reserva, visto a ocorrência de grande interferência na esfera da vida privada, que permitiu aos seus detentores conhecerem e traçarem perfis sobre hábitos de consumo, saúde, características genéticas e comportamentais de grande parte da população.

Em especial no caso do setor de seguros, a informação é insumo da atividade, tendo em vista que o risco é o elemento essencial da atividade e as informações disponíveis a respeito do bem ou da pessoa objeto do seguro são elementos que permitem analisar esse risco, determinando com maior segurança se um risco é segurável ou não e, assim, realizar a precificação do prêmio a ser pago.

O mercado de seguros é um importante setor da economia, que movimenta bilhões de reais ao ano. Para além de proteger pessoas e patrimônios, gera empregos, é contribuinte de tributos e auxilia o desenvolvimento dos mercados financeiro e de capitais.

O seguro também possui um cunho social, especialmente no cenário de crise econômica, na medida em que auxilia o governo a reduzir despesas relativas a eventos cobertos pelo seguro, como ocorre nos casos de contratação do Seguro Obrigatório de Danos Pessoais Causados por Veículos Automotores de Vias Terrestres, ou por sua carga, a pessoas transportadas ou não – Seguro DPVAT e do seguro de vida.

A utilização de dados pessoais nos contratos de seguros pode invadir a esfera da privacidade do segurado, ao valer-se de informações atinentes à sua saúde, condição econômica e hábitos pessoais, o que torna necessária a adoção de medidas que garantam um adequado grau de proteção ao direito da privacidade, sem impedir o exercício da atividade securitária.

Tais medidas devem refletir nas normas que tratam da proteção de dados ao estabelecer os parâmetros legais a serem observados, limites e direitos dos consumidores, assegurando uma maior segurança jurídica.

Entretanto, ao contrário de muitos países que já criaram regulamentação específica para a proteção de dados pessoais, com destaque para a União Europeia e os Estados Unidos, que possuem dois modelos distintos, no caso do Brasil ainda não há uma regulamentação específica.

Dessa forma, o tema ainda é tratado à luz da Constituição Federal, do Código de Defesa do Consumidor e do Código Civil, que não atende as demandas da sociedade atual.

Assim sendo, o presente estudo abordará o direito à privacidade, a tutela da proteção de dados pessoais, a legislação internacional sobre o tema, o ordenamento jurídico brasileiro, os contratos de seguro à luz dos princípios da proteção de dados pessoais e proposta de projeto de lei da Câmara dos Deputados sobre a proteção de dados pessoais.

Será feita a análise sob a ótica de como o setor de seguros poderá continuar a recolher e tratar os dados pessoais definidores de interesses seguráveis, verdadeira matéria prima da atividade securitária, garantida a proteção da privacidade dos segurados.

2. DO DIREITO À PRIVACIDADE E A TUTELA DA PROTEÇÃO DE DADOS PESSOAIS

2.1 Do direito à privacidade

No final do século XIX, durante o liberalismo jurídico clássico, a privacidade surgiu sob a perspectiva do indivíduo e do direito de ser deixado só, tendo como marco o artigo de Samuel Warren e Louis Brandeis, *The right to privacy*[1].

A tutela da privacidade nesse período tinha um viés patrimonialista, voltado exclusivamente para o indivíduo que havia tido violado o seu direito à privacidade.

Desde então a sociedade passou por muitas mudanças, que refletiram diretamente no direito à privacidade, como o surgimento dos meios de comunicação de massa, os computadores, a *internet*, proporcionando maior divulgação da informação e melhor coleta, armazenamento e processamento de dados.

Em 1948, a privacidade foi considerada como um direito fundamental previsto no rol da Declaração Universal dos Direitos Humanos da ONU.

O artigo 12 da referida Declaração dispõe: "ninguém sofrerá intromissões arbitrárias na sua vida privada, família, domicílio ou correspondência, nem ataques a sua honra e reputação, tendo contra tais intromissões ou ataques direito à proteção da lei"[2].

Além da previsão na Declaração Universal dos Direitos Humanos, a privacidade também foi reconhecida na Declaração Americana dos Direitos e Deveres do Homem[3] e na Convenção Americana de Direitos Humanos[4].

---

[1] BRANDEIS, L. D.; WARREN S. D. *The right to privacy*. Harvard Law Review, Boston, V. 4, nº 5, dec, 1890.
[2] Disponível em: < http://www.onu.org.br/img/2014/09/DUDH.pdf >. Acesso em 20 de maio de 2017.
[3] Disponível em < https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm> Acesso em 20 de maio de 2017
[4] Disponível em < https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm > Acesso em 20 de maio de 2017.

Nos referidos tratados internacionais, a privacidade é abordada como um termo amplo relacionado à proteção da autonomia individual e ao relacionamento entre indivíduo e sociedade, incluindo governos, empresas e outros indivíduos.

A partir do desenvolvimento da tecnologia e o crescimento do fluxo de informações, a privacidade passa a ser mais complexa do que a noção de isolamento, passando o seu centro de gravidade à possibilidade de cada um controlar o uso das informações que lhe dizem respeito. Então, voltam-se as atenções ara o controle por indivíduos e grupos, do exercício dos poderes fundados na disponibilidade de informações, contribuindo para um equilíbrio mais político[5].

A sociedade atual, conhecida como "sociedade da informação", é fundamentada na crença de que sua consolidação favorece a interação global nos diferentes aspectos da vida humana, na economia, no conhecimento, na cultura, no comportamento humano e nos valores[6].

Na sociedade de informação, tendem a prevalecer definições funcionais da privacidade que se referem à possibilidade de um sujeito conhecer, controlar, endereçar ou interromper o fluxo de informações que lhe dizem respeito[7].

A informação torna-se insumo tanto para a atividade empresarial, quanto para a atividade do Estado.

Por conseguinte, verificou-se uma grande dificuldade do indivíduo de saber efetivamente quem é o detentor da sua informação e como é utilizada.

Destarte, a tutela da privacidade associada ao isolamento, à reclusão, não se contextualiza em um mundo no qual o fluxo de informações aumenta incessantemente, bem como aumenta o número de violações da nossa esfera privada.

---

[5] RODOTÀ, STEFANO. *Tecnologie e diritti.* Bologna: Mulino, 1995. p. 19-20.
[6] MARTINS. Guilherme Magalhães. *O direito ao Esquecimento na Internet*. In Direito Privado e Internet. São Paulo. Atlas, 2014, p. 3-27.
[7] MARTINS. Guilherme Magalhães. *Responsabilidade Civil por acidente de consumo na internet*. São Paulo. Revista dos Tribunais, 2008, p. 238-239.

Nesse sentido, Stefano Rodotà ensina que o direito à privacidade não se estrutura mais em torno do eixo "pessoa-informação-segredo", antigo paradigma da *zero-relationship*[8], mas sim em um eixo "pessoa-informação-circulação-controle"[9].

A privacidade na sociedade de informação está relacionada ao modo como o indivíduo se apresenta com o mundo exterior, em que ele determina a sua inserção e exposição na forma das informações que ele disponibiliza.

Novamente, cita-se Stefano Rodotà, para trazer o conceito de privacidade como: "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" [10].

Ademais, na medida de em que a privacidade traduz-se no exercício do controle da informação do indivíduo, ela associa-se diretamente ao direito de liberdade, tão valorizado no Estado Democrático de Direito.

A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto a sua adequação às novas tecnologias de informação.

A proteção da privacidade na sociedade da informação busca proporcionar ao indivíduo os meios necessários para a construção e consolidação de uma esfera privada própria, em que seja assegurado o controle das suas informações e o efetivo direito de informação sobre a utilização de seus dados.

É necessário garantir que a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, para que ela não seja submetida a formas de controle social que, anulariam sua individualidade, cerceiam sua autonomia privada e inviabiliza o livre desenvolvimento de sua personalidade.

---

[8] SHILS. EDWARD. Privacy. *Its constitution and vicissitudes*. Law and contemporary problem, 2/1996, pp. 282-396.
[9] RODOTÀ, STEFANO**.** *Tecnologie e diritti.* Bologna: Mulino, 1995. p. 102.
[10] RODOTÀ, STEFANO. Op. Cit. p. 122.

2.2 O direito à privacidade no ordenamento jurídico brasileiro.

No Brasil, a Constituição Federal de 1988 assegura ao cidadão a inviolabilidade da correspondência, das comunicações telegráficas, de dados, das comunicações telefônicas, da intimidade, vida privada, honra e imagem das pessoas, bem como no caso de violação o direito à indenização pelo dano material ou moral[11].

Além disso, a Constituição Federal inseriu no art. 5º dispositivos para tutela de situações específicas, que estão dentro do escopo do direito à privacidade, como a proteção da imagem; a inviolabilidade da casa; o sigilo das correspondências e das comunicações; o direito de conhecer e retificar informações pessoais[12].

Também estabeleceu a Constituição Federal instituiu remédio constitucional, chamado de habeas data, que garante o conhecimento de informações relativas à pessoa, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público e a retificação de dados. O habeas data foi regulamentado pela Lei nº 9.507, de 1997, que dispõe sobre o direito de acesso a informações e disciplina o rito processual.

O Código Civil de 2002 elencou o direito à privacidade no rol de direitos da personalidade, onde prevê a inviolabilidade da vida privada da pessoa natural, e na hipótese de violação o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar a violação[13].

Assim, o direito à privacidade além de ser um direito fundamental constitucionalmente tutelado, também é um dos direitos da personalidade.

Os direitos da personalidade constitucionalmente tutelados são os inerentes à própria existência, elementos constitutivos da personalidade do sujeito. São direitos subjetivos, ou seja, a pessoa defende sua personalidade, e não seu patrimônio.

---

[11] BRASIL, Constituição Federal, art. 5º, incisos X e XI.
Disponível em < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm > Acesso em 26 de maio de 2017.

[12] Op. Cit. Constituição Federal, art. 5º, incisos X, XI, XII, XIV.

[13] BRASIL, Código Civil, art. 21. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm> Acesso em 27 de maio de 2017

Os referidos direitos são indisponíveis, extrapatrimoniais, absolutos, intransmissíveis imprescritíveis, impenhoráveis, vitalícios, irrenunciáveis e ilimitados[14].

Cumpre mencionar que em 2011, a V Jornada de Direito Civil, aprovou o Enunciado nº 404, que definiu importante interpretação sobre o artigo 21[15]do Código Civil. A aprovação deste enunciado ressalta a importância da inviolabilidade da vida privada da pessoa e a necessidade do expresso consentimento do indivíduo para a utilização de suas informações pessoais:[16]

> Enunciado 404 - Artigo 21: A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas.

No âmbito das relações de consumo, o Código de Defesa do Consumidor prevê que o consumidor terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes[17].

O Código de Defesa do Consumidor trouxe também obrigações para os gestores de bancos de dados, como o estabelecimento de prazo para manutenção dos dados em arquivo[18].

Há também a Lei nº 12.414 de 2011[19] - Lei do Cadastro Positivo, que estabeleceu regras para o tratamento de dados financeiros para a formação de históricos de crédito, ao prever uma série de garantias para o titular dos dados e ainda a Lei nº 12.527 de 2011[20] – Lei de Acesso a Informação, que trata sobre as garantias do acesso a informação.

---

[14] Op. Cit. Código Civil, art. 11.
[15] Op. Cit. Código Civil, art. 21.
[16] V Jornada do Direito Civil / Organização Ministro Ruy Rosado de Aguiar Jr. – Brasília: CJF, 2011. Disponível em: http://www.cjf.jus.br/enunciados/enunciado/208 . Acesso em 08 mai. 2017.
[17] BRASIL, Código de Defesa do Consumidor, art. 43. Disponível em : < http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em 08 mai.2017.
[18] Art. 43, § 1° - Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
[19] Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.
[20] Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal (1988); altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

Outrossim, em 2014 foi promulgada a Lei nº 12.968 – Marco Civil da Internet, regulamentada pelo Decreto nº 8.771, de 2016, em que a privacidade é contemplada no art. 7, I, no sentido de que "a inviolabilidade da intimidade e da vida privada assegurado o direito à sua proteção e a indenização pelo dano material ou moral decorrente da sua violação".

O Marco Civil também instituiu a preservação da autodeterminação informativa dos usuários, por meio dos arts. 8º, 10º e seguintes.[21]

O Decreto regulamentador foi o responsável pela disposição de assuntos que ainda careciam de mais atenção, sendo eles: (i) neutralidade de rede; (ii) proteção aos dados pessoais e conteúdos dos meios de comunicação privada entre os usuários; (iii) fiscalização e transparência na solicitação de dados pela administração pública e (iv) não discriminação no tráfego de pacote de dados.

Quanto à neutralidade da rede, já prevista no Marco Civil da Internet, o Decreto trouxe as hipóteses de exceção à neutralidade. Quanto à proteção aos dados pessoais, foram estabelecidas regras de requisição de dados cadastrais. As autoridades administrativas autorizadas a requisitar tais dados cadastrais, por exemplo, devem indicar o fundamento legal e a motivação do pedido.

Por fim, a legislação penal como forma de proteção do bem jurídico da privacidade tipifica os crimes contra a inviolabilidade de domicílio, a correspondência, a correspondência comercial, a divulgação de segredo e a violação de segredo profissional[22].

2.3 Informação e dados pessoais

Em relação à utilização dos termos informação e dados, vale uma observação, tendo em vista que há uma especificação técnica e semântica em cada um desses termos, ainda que o

[21] Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

[22] BRASIL, Código Penal, artigos 150 a 154. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 14 mai. 2017.

conteúdo de ambos muitas vezes se sobrepõe e são utilizados como sinônimos em alguns casos, eis que ambos os termos são para representar um fato, um determinado aspecto da realidade,

A informação pessoal é aquela se refere diretamente a um indivíduo, que está diretamente conectada com os seus direitos da personalidade, que deve observar certos requisitos para sua caracterização como tal, considerando que uma determinada informação pode possuir um vínculo objetivo com uma pessoa revelando algo sobre ela. Tal vínculo significa que a informação refere-se às características ou ações dessa pessoa, que podem ser atribuídas a ela, como o caso do nome civil ou domicílio, hábito de consumo[23].

Com efeito, é preciso que seja estabelecido esse vínculo objetivo para que seja uma informação pessoal, tendo em vista que há informações não pessoais, a exemplo da opinião alheia sobre o indivíduo ou a propriedade intelectual dele, que embora seja elaborada por ele, não é informação pessoal.

O Conselho Europeu, na Convenção de Strasbourg nº 108, de 1981 definiu informação pessoal como "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação[24]".

O termo informação refere-se em certos contextos na representação de determinados valores, como a "liberdade de informação", fundamento de uma imprensa livre, bem como seu correspectivo "direito à informação", e também do dever de informação contratual presente no dever de boa-fé objetiva na contratação em geral e, especificamente, no Código de Defesa do Consumidor.

Já o termo dado apresenta conotação mais primitiva e fragmentada, como se fosse uma informação em estado potencial, antes de ser transmitida. [25]

Os dados pessoais podem ser classificados como dados pessoais, dados sensíveis e dados anônimos. Sobre os dados sensíveis, destaca-se por Danilo Doneda que:

---

[23] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P.34

[24] Convenção nº 108 – Convenção para a proteção das pessoas com relação ao tratamento automatizado de dados pessoais, art. 2°.

[25] WACKS, Raymond. Personal information. Oxford: Clarendon Pressa, 1989, p. 25

> A prática do direito à informação deu origem à criação de uma categoria especifica de dados, a dos dados sensíveis. Estes seriam determinados tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva e que apresentaria maiores riscos potenciais que a média para a pessoa e, não raro, para a coletividade[26].

Os dados sensíveis são aqueles que estão relacionados aqueles relacionados a uma esfera absoluta da intimidade, tais como informações pertinentes à religião, preferência sexual e relação familiar, histórico médico ou dos dados genéticos.

O Regulamento da União Europeia de 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE[27], estabelece que:

> Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo origem racial no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas.[28]

Cumpre mencionar que não é apenas os dados sensíveis que estão sujeitos a ocorrência de práticas discriminatórias, mas também os dados que teoricamente não são considerados sensíveis.

Além disso, outra subespécie de dados é o dado anônimo, aquele que pode ser referir a uma pessoa indeterminada.

O dado anônimo é útil para diversas finalidades, a exemplo das informações referentes a uma determinada coletividade ou grupo específicos, sem que haja indivíduos nominados.

---

[26] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 160/ l 6 l

[27] Disponível em < http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679 > acesso em 30 de maio de 2017

[28] Op. Cit.

Tal “anonimação” de dados pessoas é a retirada do vínculo da informação com a pessoa a qual se refere.

O dado anônimo ainda pode apresentar-se útil em outras hipóteses, como aquela na qual possibilita a comunicação e expressão de sujeitos que estariam impedidos, por vínculos e limitações políticas ou sociais, de exprimir-se livremente.

Convém esclarecer que os bancos de dados tiveram origem a partir da sistematização da informação pessoal em grandes volumes, tendo seu potencial exponencialmente incrementado com o advento da informática, que tornou possível a administração de banco de dados gigantesco contendo informações pessoais.

Os bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica.

Essa lógica costuma refletir um caráter utilitarista, procurando proporcionar a extração do máximo proveito possível a partir de um conjunto de informações, que o tratamento sistematizado da informação possa gerar.

A utilidade da informação, em si, está ligada a uma série de fenômenos que cresceram em importância e complexidade nas últimas décadas.

O que hoje a destaca de seu significado histórico é uma maior desenvoltura na manipulação da informação, desde a sua coleta e tratamento até a sua comunicação.

Assim, aumentando-se a capacidade de armazenamento e comunicação de informações, cresce também a variedade de formas pelas quais ela pode ser apropriada ou utilizada.

Sendo maior sua maleabilidade e utilidade, mais ela se torna elemento fundamental de um crescente número de negócios e utilidades, aumentando a sua possibilidade de influir em nosso cotidiano, em um crescendo que tem como pano de fundo a evolução tecnológica e, especificamente, a utilização de computadores para o tratamento de dados pessoais.

Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos sobre as informações pessoais e, consequentemente, sobre a própria pessoa.

Aumenta-se então o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.

O acentuado aumento no volume de informações pessoais colhidas e passíveis de serem submetidas a tratamento introduziu, nos últimos anos, um novo paradigma no tratamento da informação.

A disponibilidade de diversos bancos de dados e de informação pessoal em volumes bastante consideráveis fez com que fossem desenvolvidos mecanismos capazes de prospectar informações não propriamente em um único banco de dados, porém em diversas fontes de informações disponíveis e, através de uma determinada sistemática que envolve o estabelecimento de correlações entre blocos de informações a princípio dispersos, gerar uma nova informação.

2.4 Da legislação internacional sobre dados pessoais

No modelo adotado nos Estados Unidos valoriza-se a liberdade, dando à privacidade um *status* quase proprietário, ao menos no que toca ao setor privado. Já na União Europeia, que tem sido mais difundido, tem como valor principal a dignidade humana, ou seja, a proteção do indivíduo é o valor mais importante.

A primeira norma internacional sobre o tratamento de dados pessoais no mundo é a Convenção nº 108, de 1981[29], do Conselho da Europa, organismo internacional que engloba, além dos 27 estados-membros da União Europeia, diversos outros países situados no continente europeu. Essa norma prevê uma série de princípios que se tornaram a base da maioria das normas de proteção de dados adotadas no mundo.

[29]Disponível em < https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm > Acesso em 18 de maio de 2017

A Convenção nº 108 foi também a base para a edição da Diretiva Europeia 95/46/CE[30], aplicável aos países membros da União Europeia e da Associação Europeia de Livre Comércio (EFTA) e que tem como foco o tratamento de dados pessoais pelo setor privado.

Há que se destacar o fato de muitos países membros da UE terem estendido as normas de proteção de dados também ao setor público quando da implementação dessa diretiva.

Outra norma adotada pela União Europeia no tema da proteção de dados é o Regulamento 45/2001[31], que cuida do tratamento de dados pessoais pelas instituições e órgãos da Comunidade Europeia.

Essa norma criou a Autoridade Europeia de Proteção de Dados, que funciona não só como um órgão regulador com relação à proteção de dados, mas também como consultoria técnica das instituições europeias que participam do processo de elaboração de leis: a Comissão, o Parlamento Europeu e o Conselho.

Existe ainda uma Diretiva nº 2002/58/CE[32], também criada pela autoridade Europeia, que traz algumas especificidades para o tratamento de dados pessoais no setor de telecomunicações.

A referida Diretiva nº 2002/58/CE, sofreu algumas alterações por documento posterior, no que toca à retenção daqueles dados. Finalmente, há, ainda, a Decisão-Quadro do Conselho 2008/977/JAI[33] (Justiça e Assuntos Internos), que regula o tratamento transfonteiriço de dados pessoais em tema de cooperação judicial e policial em matéria penal.

Ressalta-se a Carta dos Direitos Fundamentais da União Europeia[34], que, com a entrada em vigor do tratado de Lisboa,[35] em dezembro de 2009, passou a ter caráter normativo.

---

[30] Disponível em < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058> Acesso em 01/06/207

[31] Disponível em < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:pt:PDF> Acesso em 01/06/2017

[32] Disponível em < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058 > Acesso em 01/06/2017

[33] Disponível em < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32008F0977 > Acesso em 01/06/2017

[34] Disponível em < http://www.europarl.europa.eu/charter/pdf/text_pt.pdf> Acesso em 01/06/2017

A Carta traz pela primeira vez para o ordenamento europeu o entendimento da proteção de dados como um direito fundamental autônomo, diferente do direito à privacidade, também contemplado pela carta.

Por fim, a norma de maior relevância na União Europeia é a Diretiva 95/46[36], que traz alguns conceitos e regras importantes para o tratamento de dados, como os conceitos de dados pessoais e sensíveis, os princípios que regem o tratamento de dados – finalidade, proporcionalidade e informação – e os direitos dos titulares dos dados – consumidores – quanto ao acesso, retificação, bloqueio e exclusão.

Em seu artigo 25, a diretiva estabelece a regra da adequação, segundo a qual uma empresa situada em um país membro da União Europeia só pode transferir dados pessoais para um país fora do território da União se esse país terceiro garantir um nível de proteção de dados adequado segundo os padrões europeus.

Caso contrário, cada transação de remessa de dados deverá ser coberta por um contrato que assegure um nível de proteção adequado garantido por cláusulas padrão aprovadas pela Comissão Europeia, o que encarece, em muito, o custo dessas operações de transferência de dados.

Por fim, destaca-se que referida Diretiva foi revogada em abril de 2016 pelo Regulamento (UE) 2016/679 do Parlamento e do Conselho[37], que entrará em vigor em maio de 2018.

Além do Regulamento foram criados:

a) Diretiva (UE) 2016/680[38] do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados

---

[35] Disponível em < https://www.parlamento.pt/europa/Documents/Tratado_Versao_Consolidada.pdf > Acesso em 01/06/2017

[36] Disponível em < http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:31995L0046 > Acesso em 01/06/2017.

[37] Disponível em < http://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32016R0679 > Acesso em 01/06/2017

pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados;

b) Diretiva (UE) 2016/681[39] do Parlamento Europeu e do Conselho, relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave. São textos longos, densos, complexos que carecem de espaço para formação e reflexão.

Além disso, foram alterados e introduzidos novos conceitos com relação:

a) A introdução de um conceito de "violação de dados pessoais";
b) Ao tratamento desenvolvido da pseudoanonimização;
c) Ao direito a ser esquecido;
d) Ao direito à portabilidade dos dados;
e) "*privacy by design*";
f) "*privacy by default*";
g) As avaliações de impacto sobre proteção de dados;
h) Ao responsável pela proteção de dados[40].

2.5 A Proteção de dados pessoais

A proteção de dados pessoais é tida em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana, sendo considera inclusive como um direito fundamental.

Nesse sentido é o Regulamento da União Europeia de 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados determina que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental.

---

[38] Disponível em < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680 > Acesso em 01/06/2017

[39] Disponível em < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0132.01> Acesso 01/06/2017

[40] Disponível em < https://www.icjp.pt/cursos/8879/pdf> Acesso 05 de junho de 2017

Além disso, Carta dos Direitos Fundamentais da União Europeia e o do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelece que toda pessoa tem direito à proteção dos dados de caráter pessoal que lhes digam a respeito.

Também a proteção de dados pessoais é reconhecida pelo Conselho de Direitos Humanos da ONU como parte fundamental da privacidade pelo artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos[41].

O art. 17 dispõe que ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação e que toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

Em seu Comentário Geral, o órgão declarou que a coleta e a manutenção de informações pessoais em computadores, bancos de dados e outros dispositivos, seja por autoridades públicas ou indivíduos ou órgãos privados, devem ser regulados por lei, por meio de medidas efetivas.

Tais medidas devem ser tomadas pelos Estados para assegurar que informações relativas à vida privada de uma pessoa, para que não fiquem em poder de pessoas não estão autorizadas por lei para recebê-las, processá-las e usá-las, assim como nunca serem usadas para propósitos incompatíveis com o Pacto.

Entretanto, o direito à proteção de dados pessoais não é absoluto e deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o principio da proporcionalidade.

Cumpre mencionar que no ordenamento jurídico brasileiro ainda não há uma regulamentação específica sobre o tratamento de dados pessoais, somente é assegurado ao indivíduo o direito da privacidade.

[41] Disponível em < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm > Acesso em 05/06/2017

Dessa forma, a proteção de dados ainda deve ser analisado à luz da legislação vigente, ou seja da Constituição Federal e das legislação infra legais.

Segundo Danilo Doneda, a proteção de dados pessoais é:

> Em suma, a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém não limitada por esta, e que faz referência a um leque de garantias fundamentais que se encontram no ordenamento brasileiro[42].

É por meio da proteção de dados pessoais, que as garantias que eram relacionadas com a privacidade passam a ser vistas sob a ótica mais abrangente, pela qual outros interesses devem ser considerados, compreendendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais.

Estes interesses devem ser observados pelo operador do direito por tudo que representam, e não somente pelo seu traço visível – a violação da privacidade – para uma completa apreciação do problema.

Verificou-se então a necessidade de assegurar a autonomia e liberdade individual na sociedade de informação.

O tratamento de dados pessoais na sociedade de informação, em especial por processos automatizados representa grandes riscos ao indivíduo e ofensa à sua privacidade.

Tal risco se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, que pode ser no uso por terceiros sem o conhecimento ou autorização de seu titular, em dados incorretos representando erroneamente o titular, e até mesmo para fins discriminatórios.

Além disso, surge a necessidade na sociedade de informação de criação de instrumentos, que assegurem o indivíduo o efetivo conhecimento e controle sobre seus próprios dados. Ressalta-se que estes dados tem relação direta com a própria personalidade do indivíduo.

---

[42] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 326

Há mais de vinte anos, o Ministro Ruy Rosado de Aguiar, no âmbito do Recurso Especial nº 22.337/RS no Superior Tribunal de Justiça - STJ identificou que:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer saber da existência de tal atividade, ou não dispõe de eficazes meios para conhecer seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imerso de atos da vida humana praticados através da mídia eletrônica ou registrado nos disquetes de computador.[43]

Visto que a informação se transforma em insumo da produção em um modelo econômico voltado para a individualização e especialização dos consumidores. O setor privado armazena e processa grande quantidade de informações quase cotidiana dos consumidores e de seus hábitos de consumo, ampliando os riscos à violação da personalidade do consumidor.

O consumidor por ser polo vulnerável da relação possui grande dificuldade de controlar o fluxo de dados e de informações pessoais no mercado, bem como de adotar medidas de autoproteção contra os riscos desse processamento.

A enorme importância que os dados pessoais adquiriram no mercado de consumo atual pode ser explicada com a crise da produção em massa e o surgimento da economia de especialização flexível, que se caracteriza pela diversificação da produção para diferentes produtos e diferentes clientes.

---

[43] STJ, Recurso Especial nº 22.337/RS, Relator Ministro Ruy Rosado de Aguiar. Disponível em: https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=3&formato=PDF . Acesso em 18 mai. 2017.

A utilização de dados pessoais em diversas atividades não é, em si, um problema. Na verdade, ela torna possíveis certas empreitadas com um alto grau de eficiência, em áreas que vão do planejamento administrativo à pesquisa de mercado.

Ocorre que esta atividade requer instrumentos que a harmonize com os parâmetros de proteção da pessoa humana ditados pelos direitos fundamentais, instrumentos que possibilitem aos interessados um efetivo controle em relação aos seus dados pessoais, garantindo o acesso, a veracidade, a segurança, o conhecimento da finalidade para a qual serão utilizados.

Na proteção de dados pessoais não é somente a privacidade que deve ser tutelada, mas também a pessoa deve ser tutelada contra o controle indevido e contra a discriminação, isto é, em aspectos fundamentais de sua própria liberdade pessoal.

Além disso, e não é mais a pessoa humana, considerada individualmente, a ser a única a atingida, antigo paradigma do direito à privacidade, mas inteiras classes e grupos sociais.

Exemplo disso se dá justamente na análise de dados de classes e grupos sociais que se baseia a precificação do seguro.

Assim sendo, o tratamento da proteção de dados pessoais de forma autônoma é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos.

Os desdobramentos e efeitos do tratamento automatizado de informações pessoais, mais do que justificam mudanças e atualizações pontuais no ordenamento jurídico, formando as bases daquilo que vem sendo tratado, hoje, como um direito fundamental à proteção de dados.

O amadurecimento desse direito observa-se no decorrer das cerca de quatro décadas que a disciplina da proteção de dados pessoais ostenta.

A mudança do enfoque dado à proteção de dados nesse período pode ser brevemente entrevisto na classificação evolutiva das leis de proteção de dados pessoais realizada por

Viktor Mayer-Scönberger, que vislumbra quatro diferentes gerações de leis que partem desde uma primeira geração, cujo enfoque era mais técnico e restrito aos grandes[44].

A falta de experiência no tratamento com tecnologias ainda pouco acessíveis, aliada ao receio de um uso indiscriminado dessa tecnologia, sem que se soubesse ao certo suas consequências, fez com que, não raro, fossem preferidos princípios de proteção bastante abstratos e amplos, focalizados basicamente na atividade de processamento de dados, além de regras concretas e específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados.

Esse enfoque era natural, visto a motivação de essas leis terem sido uma "ameaça" representada pela tecnologia e, especificamente, pelos computadores.

A estrutura e a gramática dessas leis eram algo tecnocrática e condicionada pela informática – nelas, tratava-se dos "bancos de dados", e não propriamente da "privacidade", desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, a serem determinados ex ante, sem considerar a participação do cidadão de maneira mais concreta nesse processo.

O artigo "*Privacy and freedom*"[45], de Alan Westin, foi o marco em que surge torno da privacidade, do modelo de definição baseado na autodeterminação informativa. Nele, identificam-se quatro estados básicos da privacidade: solidão, reserva, anonimato e intimidade e classifica as ameaças à privacidade em vigilância física, vigilância psicológica e controle de dados.

Dessa forma, o direito a privacidade vai evoluindo para garantia a proteção dos vários aspectos da privacidade, se dividindo em gerações até a forma da legislação internacional atual.

---

[44] MAYER – SCONBERGER, Viktor. "General development of data protection in Europe", in Technology and privacy: Thechnology and privacy: The new landscape. AGRE, Phillip; ROTENBERG,Marc, (orgs). Cambridge: MIT Press, 1997, pp. 219-242 apud, DONEDA, 2006. p. 352.

[45] WESTIN, Alan, Privacy and freedom, new York: Athencum, Signet, 1972, pp. 259-260, apud DONEDA, 2006, p. 161

As leis de primeira geração propunham-se a regular um cenário no qual se preocupavam basicamente no Estado como detentor dos seus dados, como administradores de banco de dados.

Já a partir da década de 1970, surge a segunda geração das leis de proteção de dados pessoais, que é baseada na consideração da privacidade e proteção dos dados pessoais como uma liberdade negativa, a ser exercitada pelo próprio cidadão, que se dá pela identificação do uso indevido de suas informações e sua tutela.

Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão – ou seja, a atuação direta da "liberdade" do cidadão de interromper o fluxo para o exterior de suas informações pessoais – implicava não raro na sua exclusão de algum aspecto da vida social, ou em algum tipo de prejuízo mensurável.

Na década de 1980, forma-se uma terceira geração de leis, que continua sendo centrada no cidadão, porém passa a abranger mais do que a liberdade de fornecer ou não seus dados pessoais, mas preocupando-se também em manter a efetividade desta liberdade.

A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – e assim proporcionando o efetivo e pleno exercício da autodeterminação informativa.

A autodeterminação informativa, de fato, surgiu basicamente como uma extensão das liberdades presentes nas leis de segunda geração, e são várias as mudanças específicas neste sentido que podem ser identificadas na estrutura destas novas leis.

O tratamento de dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa para a utilização de seus dados pessoais, porém procurava fazer com que a pessoa participasse consciente e ativamente nas fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros; estas leis incluem garantias específicas como o dever de informação.

As leis de quarta geração, são as que existem hoje em vários países, caracterizam hoje por suprir as desvantagens do enfoque individual existente até então. Nelas percebe-se a consciência do problema integral da informação na fundamentação da disciplina, que implica no fato de que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessárias instrumentos que elevem o padrão coletivo de proteção. Neles está presente igualmente uma forte dose de pragmatismo, voltado para a busca de resultados concretos.

Entre as técnicas utilizadas pelo legislador na elaboração de leis estão o fortalecimento da posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação, que não era resolvido com medidas que simplesmente reconheciam o direito à autodeterminação informativa; outra, paradoxalmente, é a própria redução do papel da decisão individual na autodeterminação informativa.

Isto ocorre porque se parte do pressuposto que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, que não pode ser obtida exclusivamente de uma decisão individual.

Outras características são a disseminação do modelo das autoridades independentes para a atuação da lei – tanto mais necessárias com a diminuição do poder de "barganha" do indivíduo para a autorização ao processamento de seus dados; e também surgimento de uma normativa conexa, tal como as normas específicas para alguns setores de processamento de dados.

> A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito.
>
> Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida.
>
> Qualquer registro, divulgação e utilização de informações pessoais fora destes procedimentos não devem ser permitidos, por consistirem em uma prática desleal, a não se que tal registro, utilização ou divulgação sejam autorizados por lei. [46]

[46] E.U.A. Records, computers and the rights of citizens. Report of the Secretar`s Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: <aspe.hhs.gov/datacnc1/1973privacy/c3.htm> DONEDA, 2006, p. 304

Assim ensina DONEDA, que uma concepção como esta necessita que sejam determinados meios que resguardem o cidadão, que efetivamente vieram descritos como:

> - Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo".
> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de que forma ela é utilizada.
> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de que forma ela é utilizada.
> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de que forma ela é utilizada.
> - Deve existi um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito[47]

Danilo Doneda também ensina que:

> "Toda organização que crie, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados [48]."

Destaca-se que tais regras devem ser de caráter marcantemente procedimental, constituindo um conjunto de medidas que passou a ser encontrado em diversos normativos sobre proteção de dados pessoais.

Este núcleo comum encontrou expressão como um conjunto de princípios a ser aplicados na proteção de dados pessoais na Convenção de Strasbourg e nas Guidelines da OCDE, no início da década de 1980. Podemos, a este ponto, elabora uma síntese destes princípios:

> 1. **Princípio da publicidade (ou da transparência)**, pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pelo notificação de sua criação a uma autoridade; ou pela divulgação de relatórios periódicos.
> 2. **Princípio da exatidão:** Os dados armazenados devem ser fieis à realidade, o que compreende a necessidade que sua coleta e seu tratamento sejam feitos com cuidado e correção, e que sejam realizadas atualizações periódicas destes dados conforme a necessidade.
> 3. **Princípio da finalidade,** pelo qual toda utilização dos dados pessoais devem obedecer à finalidade comunicada ao interessado antes da sua coleta. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

---

[47] DONEDA, Danilo. Revista Brasileira de Risco e Seguro, Rio de Janeiro, v. 5. N. 10, out. 2009/mar. 2010 Disponível em: < http://www.rbrs.com.br/arquivos/RBRS10-4%20Danilo%20Doneda.pdf> . Aceso em 18 mai. 2017.

[48] DONEDA, Danilo. Op. cit., p. 96

> 4. **Princípio do livre acesso,** pelo qual o indivíduo tem acesso ao banco de dados, no qual suas informações estão armazenadas, podendo obter cópias destes registros com a consequente possibilidade de controle destes dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou ainda pode-se procede a eventuais acréscimos.
> 5. **Princípio da segurança física e lógica,** pelo qual dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado." [49]

Estes princípios, mesmo que fracionados, condensados ou então adaptados, podem ser identificados em diversas leis, tratados, convenções ou acordos entre privados.

Eles são o núcleo das questões com as quais todo ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção de dados pessoais.

A aplicação de tais princípios, no entanto, é a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e a sua consideração como um direito fundamental em diversos ordenamentos.

[49] DONEDA, Danilo. Op. cit., p. 93

3.0 A INFORMAÇÃO E OS CONTRATOS DE SEGURO

O desenvolvimento tecnológico contribuiu para a coleta, armazenamento e utilidade dos dados para diversos fins, tornando a informação um bem, ligado à pessoa, mas capaz de ser utilizada sem o seu conhecimento e autorização.

Neste sentido, a informação pessoal é o elemento fundamental em uma série de novos modelos de negócios típicos da Sociedade da Informação, sobretudo para o setor de seguros.

Sobre o setor de seguros, cumpre tecer algumas considerações.

O contrato de seguro é o instrumento pelo qual o segurador se obriga, mediante o pagamento do prêmio, a garantir o interesse legítimo do segurado, relativo à pessoa ou a coisa, contra riscos predeterminados[50], que é caracterizado como um contrato bilateral, oneroso, aleatório, de adesão, de execução continuada, consensual e de máxima boa-fé.

Entende-se por interesse legítimo do segurado, seja pessoa natural ou jurídica, a proteção econômica quanto à vida de uma determinada pessoa ou um bem.

Logo, o objeto do contrato de seguro é o interesse segurável, relativo aos bens descritos na apólice, em que se aplica uma valoração econômica.

Em outras palavras, o interesse legítimo é a relação lícita de valor econômico sobre um bem. Caso essa relação seja ameaçada por um risco, há um interesse legítimo segurável, que vem a ser o objeto de qualquer contrato de seguro, seja ele de dano ou de pessoa.

Outrossim, o segurado contrata o seguro para garantir esse interesse contra perdas decorrentes de riscos predeterminados.

---

[50] Art. 757. Pelo contrato de seguro, o segurador se obriga, mediante o pagamento do prêmio, a garantir interesse legítimo do segurado, relativo a pessoa ou a coisa, contra riscos predeterminados. Código Civil (2002). Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm> . Acesso em 18 mai. 2017.

Tal instrumento encontra-se previsto nos artigos 757 a 802 do Capítulo XV do Código Civil, que estabelece as normas gerais dessa espécie de contrato.

Além disso, todas as operações de seguros privados realizadas no país estão sujeitas às disposições do Decreto-Lei nº 73/1966 e de leis especiais, como a Lei nº 8.078/90 - Código de Defesa do Consumidor.

Sobre o Decreto-Lei nº 73/66, destaca-se que é um setor regulamentado pelo Conselho Nacional de Seguros Privados – CNSP e a Superintendência de Seguros Privados.

O risco, cuja ocorrência independe da vontade das partes contratantes, nada mais é do que a expectativa de ocorrência do sinistro (evento incerto previsto no contrato de seguro e por ele coberto), razão pela qual a depreciação gradativa, insidiosa do bem, não integra o conceito do risco.

Para a precificação do risco e definição do valor do seguro, são realizados cálculos atuariais que avaliam a probabilidade de materialização dos riscos. É com base nas estatísticas e nos cálculos atuariais que se constata a probabilidade de determinado evento danoso vir a ocorrer.

Tais cálculos são baseados na informação pessoal, que são coletadas pela sociedade seguradora para a definição do valor do prêmio. Entretanto, é preciso se atentar para que na precificação do seguro, a seguradora não se utilize de critérios discriminatórios, em especial quanto aos dados sensíveis.

Sobre a coleta da informação pessoal, o disposto no art. 766 do Código Civil, prevê que o segurado ou o seu representante são obrigados a fazer declarações exatas e completas à seguradora, inclusive de todas as circunstâncias que possam influir na aceitação da proposta ou no cálculo do prêmio.

Ressalta-se que as declarações do segurado são o insumo para as seguradoras calcularem a probabilidade de ocorrência do sinistro e o valor do prêmio do seguro.

Assim sendo essas declarações são de fundamental importância para as seguradoras, e o segurado deve manter uma conduta de transparência, dentro do princípio da boa-fé, sob pena de perder o direito à garantia, se comprovado que omitiu informações ou procedeu de má-fé quando de suas declarações.

Destaca-se que se trata de um contrato de extrema boa-fé, conforme expressamente previsto no art. 765 do Código Civil, que assim dispõe:

> Art. 765. O segurado e o segurador são obrigados a guardar na conclusão e na execução do contrato a mais estrita boa-fé e veracidade, tanto a respeito do objeto como das circunstâncias e declarações a ele concernentes.[51]

Também o Código de Defesa do Consumidor estabelece o segurador como fornecedor de serviços, ressaltando a incidência da boa-fé nas relações securitárias.

O contrato de seguro baseia-se, portanto, numa relação de confiança entre o segurado e a seguradora. Ambos devem agir, nas tratativas, na conclusão e durante a execução do contrato, com boa-fé, lealdade e veracidade.

A primeira forma de coleta de dados pela sociedade seguradora ocorre no momento da emissão da apólice, em que dispõe o art. 759 do Código Civil, que a mesma deverá ser precedida de proposta escrita, contendo a declaração dos elementos essenciais do interesse a ser garantido e do risco assumido pela seguradora.

Ora, é justamente pelo cálculo atuarial que nota-se importância da informação para o setor de seguros. O cálculo de estatísticas e probabilidades avalia a eventual ocorrência de riscos mediante dados pessoais, como sexo, idade, hábitos.

Pode-se citar como exemplo o seguro de automóvel, em que jovens pagam um preço maior, por ser estatisticamente comprovado, que estão sujeitos a maiores riscos.

---

[51] Código Civil (2002). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm> . Acesso em 18 mai. 2017.

A precificação a partir das informações pessoais torna o preço do seguro mais equilibrado, na medida em que de fato o indivíduo paga pelo risco que está sujeito. Ao contrário fosse, ocorreria uma divisão em que os indivíduos sujeitos a menores riscos poderiam pagar a mais, inibindo a contratação do seguro por esses indivíduos.

Cabe esclarecer que tais práticas tem origem no fenômeno da assimetria de informação, que ocorre quando dois ou mais agentes econômicos estabelecem entre si uma transação econômica com uma das partes envolvidas detendo informações que qualificam ou quantitativa superiores aos da outra parte.

A assimetria de informações no mercado de seguros afeta tanto segurados quanto seguradores, tendo em vista que cada parte tem superioridade informacional sobre a outra em determinados aspectos e inferioridade informacional em outros.

É certo que há grande dificuldade, inclusive técnica, para dar o amplo acesso da forma como a seguradora precifica os dados pessoais.

Da assimetria de informação, gera o risco moral, pois o segurado pode ter omitido dados relevantes para a seguradora, ou seja, há mudança em seu comportamento após ter contratado o seguro, com o consequente agravamento do risco.

Se for omissão consciente, há quebra do principio da máxima boa-fé, conforme exposto, norteia os contratos de seguros.

Tal princípio não objetiva apenas garantir honestidade no suprimento de informações entre segurado e segurador, mas impõe o dever das partes de revelar plenamente entre si qualquer fato que entendam ser relevante para a contratação da apólice, seja objetivo (material) ou subjetivo.

Outra situação em decorrência da assimetria de informação é a seleção adversa, que surge quando as seguradoras têm dificuldade para distinguir o risco, em que apenas os consumidores de alto risco permanecem contratando o seguro, criando-se um déficit para os de baixo risco.

É evidente que cada segurado tem um perfil de risco diferente do outro. Contudo, não há como as seguradoras diferenciarem o risco com grande detalhamento, nem seria razoável fazê-lo. Assim, a seguradora precifica com base em riscos definidos para classes ou grupos inteiros de segurados.

A soma dos prêmios pagos por pessoas sujeitas aos mesmos riscos ou a riscos semelhantes permite à seguradora formar um fundo, por ela administrado, que fará frente ao pagamento das indenizações aos segurados ou do capital ao segurado ou beneficiário.

A esse respeito, é importante esclarecer que a atividade seguradora é exercida sob o mutualismo, princípio que exprime um regime de cooperação, de contribuição coletiva que leva um grupo de segurados expostos aos mesmos ou a riscos semelhantes a aportar somas para a formação de um fundo que irá repor a perda futura, incerta e eventual de alguns segurados.

Assim, pessoas que se encontram sob riscos iguais ou semelhantes são reunidas para contribuir para esse fundo, que suportará as perdas eventuais de alguns, nos valores e limites previstos no contrato de seguro, competindo à seguradora zelar pela proteção dos segurados, na qualidade de gestora da mutualidade.

É importante destacar que o contrato de seguro é um contrato por adesão, pois no momento de sua celebração, caberá ao segurado aderir ao que lhe é proposto. Os contratos de seguro são padronizados, sendo suas condições gerais são previamente aprovadas pela Susep.

A classificação do contrato de seguro como de adesão, terá influência ser analisado o consentimento do indivíduo na utilização de seus dados, na medida em que não há como o indivíduo negar a disponibilização da informação exigida, pois se não consentir o fornecimento da informação solicitada, não poderá contratar o seguro.

Por fim, por tratar de um setor regulamentado, quanto à proteção de dados destaca-se a Resolução CNSP nº 294/13[52] que dispõe sobre a utilização de meios remotos nas operações relacionadas aos planos de seguro e de previdência complementar aberta.

[52]Disponível em: http://www2.susep.gov.br/bibliotecaweb/docOriginal.aspx?tipo=1&codigo=31432 Acesso em 18 mai. 2017.

A referida Resolução prevê a identificação do proponente/contratante, assegurando a autenticidade, a confidencialidade e a integridade de seus dados, a segurança na troca de dados e informações com o proponente/contratante ou, quando couber, com o corretor, e que os dados cadastrais dos proponentes e contratantes não poderão ser objeto de cessão a terceiros, ainda que a título gratuito, e a sua utilização ficará restrita aos fins contratuais.

Em suma, apesar da Resolução não ser específica quanto à proteção de dados pessoais, ela busca assegurar ao consumidor maior proteção aos seus dados no momento da contratação eletrônico dos seguros.

3.1. O contrato de seguro à luz dos princípios da proteção de dados pessoais

O tratamento de dados no contrato de seguro somente poderá ocorrer mediante o consentimento livre informado e inequívoco, que significa dizer que o indivíduo deve saber exatamente o propósito da coleta do seu dado e a destinação que será dada a tal informação

Todavia, os contratos de seguro, conforme exposto que são contratos de adesão, em que é praticamente impossível para o contratante se negar a prestar a informação exigida pela seguradora, mesmo que não esteja em situação de vulnerabilidade, pois se não consentir o fornecimento da informação solicitada, não poderá contratar o seguro.

Destaque-se que o próprio Código Civil, em seu art. 766, obriga o segurado a prestar todas as informações que possam influir na aceitação da proposta ou na taxa do prêmio, sob pena de perder a garantia se omiti-las por má-fé.

Neste sentido, Teresa Negreiros comenta como ocorre o consentimento nos contratos de adesão, tendo como um dos exemplos apresentados o contrato de seguros:

> O contrato de adesão tem por objeto a aquisição e utilização de toda a sorte de bens, de eletrodomésticos a prestação de serviços públicos, de atividades financeiras - bancárias e de seguro - a serviços de transportes, em suas mais variadas

> modalidades. Caracteriza-se pelo modo de sua formação: O consentimento manifesta-se com a simples adesão a conteúdo preestabelecido da relação jurídica[53].

Contudo, ressalta-se que o indivíduo precisa ser informado quanto às possíveis destinações de seus dados.

Essa necessidade de que o consentimento seja informado para que tenha eficácia já se correlaciona com a importância dos princípios da finalidade e da transparência, na medida em que para o consentimento ser efetivo deve o segurado ter as informações para qual fim será utilizada a informação e de que forma, no momento da coleta.

O princípio da finalidade funciona como um limitador do consentimento, ou seja, ele afasta a generalidade que este pode apresentar, fazendo com que a utilização dos dados pessoais seja para um fim ou fins específicos[54].

Já o princípio da transparência é um complemento necessário do princípio da finalidade, pois ele impõe ao coletor do dado, no caso a seguradora, o dever de informar ao interessado, prestando-lhe toda informação necessária com relação ao destino que será dado aos seus dados pessoais, o que inclui a que se destina, para qual finalidade serão utilizados, por quanto tempo, quem terá acesso aos seus dados, se estes dados poderão ser transmitidos a terceiros, e mais tantos outros detalhes quanto seja, necessários em urna determinada situação, para que o interessado possa formar sua convicção, livre e consciente, para realizar o ato de autodeterminação.

Aliás, esse dever de informação nos contratos de consumo já provém do próprio Código de Proteção Defesa do Consumidor, que estabelece como direito básico do consumidor "a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentem[55]".

---

[53] NEGREIROS, Teresa. Fundamentos para uma interpretação constitucional do princípio da boa-fé. Rio de Janeiro, Renovar, 2002, p. 360

[54] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.p 383.

[55] Art 4º do Código de Defesa do Consumidor. Disponível em: >http://www.planalto.gov.br/ccivil_03/leis/L8078.htm> Acesso em 18 mai. 2017.

Na verdade, o consentimento é necessário e deve existir, porém ele é apenas um primeiro elemento[56], que deve ser acompanhado de outros elementos para que o dado possa vir a ser coletado e utilizado.

Retornando ao conceito do contrato de seguro como adesão, conclui-se que, o consentimento puro e simples não pode funcionar como único elemento a autorizar a coleta e utilização de dados pessoais na contratação de seguros, uma vez que ele deveria ser livre e esclarecido.

É evidente que atualmente a maior parte dos consumidores não detém do devido conhecimento quanto à utilização de seus dados no contrato de seguro. No momento da contratação não é devidamente informado sobre o uso de dados. Inclusive, alguns dados são coletados sem o conhecimento do segurado para tal, a exemplo do acesso ao banco de dados restritivos ao crédito.

Em outras palavras, a seguradora tem o dever de informar ao potencial ou atual segurado quem terá acesso a seus dados e se esses dados poderão ser transferidos ou disponibilizados para terceiros.

Há também casos de criação de uma base de dados com a integração dos cadastros das empresas de seguros, que deveria ter previamente o expresso consentimento dos titulares dos dados ali contidos, o que não ocorre.

Quanto ao princípio da adequação, dele se extrai que o dado coletado deve ser compatível com a finalidade a que se propõe, ou seja, a seguradora não poderá, por exemplo, ao exigir em uma proposta de seguro celular que o proponente informe se possui carro ou computador em casa; por outro lado, em um seguro de automóvel, não se poderá exigir que a pessoa preenchesse uma declaração de saúde.

Isso cria para o coletor do dado, no caso a seguradora, o dever de identificar todos os potenciais fins para os quais o dado pessoal possa vir a ser processado, e assegurar que o titular do dado seja comunicado adequadamente das suas potenciais destinações[57] .

[56] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.p. 378

Portanto, se a seguradora coletar dado de um segurado para fins de celebração de um contrato de seguro, não poderá, posteriormente, disponibilizar esse dado para outra empresa do mesmo grupo financeiro, por exemplo, um banco, para que este venha a utilizar esse dado em contrato de empréstimo, caso não tenha informado o titular do dado sobre essa possibilidade[58].

Ressalte-se que o dado a ser transmitido ou disponibilizado para terceiros deve estar relacionado diretamente ao objeto do contrato celebrado entre seu titular e o coletor inicial do dado, sendo certo que esse dado também deve ser destinado a fins semelhantes, como, por exemplo, um contrato entre o titular do dado e o terceiro, além do fato desse dado ter que ser compatível com o objeto do novo contrato.

Dessa forma, o dado deve ser utilizado para fim específico, compatível com o objeto do contrato, e tal fim deve ser informado previamente ao titular do dado, no caso o consumidor-segurado, não sendo aceito o consentimento genérico ou aparente para toda e qualquer utilização de dado pessoal, [59]nem tampouco em consentimento tácito.

Sobre o princípio do livre acesso, esclarece-se que o primeiro dos direitos do potencial ou atual segurado, com relação à armazenagem de seus dados pessoais, é o de tomar conhecimento de que alguém começou a estocar informações a seu respeito, independentemente de provocação ou aprovação sua.

Esse dever de comunicação já se encontra previsto no direito básico e genérico estatuído no art. 62, e, mais especificamente, no art. 43, §2º, ambos do Código de Defesa do Consumidor, em que permite ao consumidor a possibilidade de retificar ou ratificar o registro.

Tal princípio encontra-se vinculado à retificação de seus dados pessoais em arquivos ou bancos de dados é aquele que lhes possibilita o acesso às informações neles armazenadas.

---

[57] CAREY, 2004, Op. Cit. p. 54.
[58] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.p, p. 339.
[59] DONEDA, Danilo. Op. Cit. p. 383

Dessa forma, poderá o segurado, a qualquer momento, exigir da seguradora ou do gestor da base de dados o acesso a seus dados armazenados e, sendo constatada qualquer irregularidade nas informações ali mantidas, terá o consumidor o direito de exigir a sua imediata retificação.

Caso a seguradora ou gestora da base de dados se recuse a dar acesso às informações ou a retificá-las, na hipótese de o consumidor-segurado encontrar alguma incorreção, poderá este se valer não só das vias judiciais ordinárias, por força do disposto do art. 43 do Código de Defesa do Consumidor, como também do *habeas data*, nas hipóteses previstas no art. 51, inciso LXXII da Constituição da República de 1988.

Além disso, quanto ao princípio da não discriminação, em que o tratamento de dados não pode ser realizado para fins discriminatórios, não deve ser confundido com a precificação de seguros, sobretudo quando da utilização dos dados sensíveis.

No caso dos dados sensíveis, em razão de sua potencial utilização discriminatória e lesiva do foro íntimo, necessitam de proteção diferenciada daquela aplicada aos demais tipos de dados pessoais.

Há quem defenda que o armazenamento e utilização de todo e qualquer dado sensível constituí ato ilícito[60]

Essa, entretanto, não parece à solução mais adequada para o problema e, conforme já dito anteriormente é necessário buscar um ponto de equilíbrio, onde se preserve a dignidade humana, através da proteção da privacidade, sem, de outro lado, inibir a autonomia da vontade, com a livre iniciativa, o que não é alcançado com a vedação total da utilização de tais dados.

No caso do contrato de seguro há situações nas quais a coleta e a utilização de dados sensíveis se faz necessárias, mas é evidente que não é todo e qualquer dado, seja ele sensível ou não, que pode ser coletado e utilizado para fins de precificação de seguros.

[60] GONÇALVES, Maria Eduarda, *Direito da informação*. Coimbra: Almedina, 1995.

Não deve ser aceito para a precificação de seguros a utilização de dados relativos à opção sexual, à orientação religiosa e à etnia, por apresentar um potencial discriminatório elevadíssimo.

Além disso, essa sua influência no risco seria demasiadamente subjetiva, não se justificando a utilização de tais dados, sob pena de impor aos seus titulares um ônus excessivo, no sentido de fazerem prova negativa da existência desse aumento de risco, o que provocaria uma exposição inaceitável de sua privacidade.

O tratamento do dado sensível demanda uma análise casuística das situações nas quais se pretende coletá-lo ou utilizá-lo, não se podendo afirmar a priori e de forma genérica que certo tipo de dado sensível poderá ser utilizado.

Um caso prático da forma como o tratamento de dados pessoais impactou o setor de seguros e aos consumidores, aconteceu em 2011 quando o Tribunal de Justiça da União Europeia no caso "*Test Achats*[61]" decidiu pela proibição da utilização de informação sobre gênero para fins de diferenciação de prêmios nos contratos de seguro por considerar discriminatório e ofender o princípio da igualdade entre os gêneros.

A decisão proferida pelo Tribunal, sob a premissa de se estar protegendo o direito fundamental à igualdade, especialmente a igualdade de gênero, na prática, gerou indesejáveis efeitos sob o mercado de seguros europeu, haja vista que, proibidas de adotar o gênero como critério de avaliação de risco contratual o qual reduzia o valor dos prêmios e prestações dos contratos de seguro de automóvel e renda celebrados com mulheres, as empresas de seguro se viram obrigadas a promover o aumento do valor dos prêmios e prestações, afetando diretamente este grupo de seguradas, que ao pagarem prêmios desproporcionais aos riscos de seu contrato, estão financiando os prêmios daqueles contratos de maior risco, o que configuraria um tratamento desigual.

Além do efeito direto sob os contratos de seguros celebrados com pessoas do sexo feminino, foi possível constatar risco de impactos econômicos sobre os demais contratos de seguro, decorrente dos custos que estas empresas terão que suportar para reavaliar todo o seu

[61] Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52012XC0113%2801%29 Acesso em 18 mai. 2017.

sistema de dados e cálculos atuariais, alterar os contratos vigentes, modificar seu material publicitário, dentre outros, custos que indubitavelmente serão repassados aos consumidores, impactando nos preços dos produtos ofertados.

Sem contar as ineficiências econômicas geradas para todos setores do mercado, decorrentes da substituição do critério sexo por outros relacionados aos hábitos de vida do segurado, cuja investigação, além de mais custosa, poderá representar uma violação à intimidade do contratante.

Mister se faz ressaltar que o gênero do segurado é fator importante para aferição do risco, visto que estatisticamente a mulher está menos exposta a certos riscos do que os homens estão, tais como o de sofrer um ataque cardíaco ou de morte prematura (a mulher tem uma expectativa de vida maior que a do homem), ou mesmo de se envolver em um acidente de trânsito, o que por si só já justificaria o tratamento diferenciado.

Assim, utilizar o gênero como um fator de diferenciação de aferição de preços em seguros tem uma lógica, já que as mulheres efetivamente apresentam um risco menor, estatisticamente demonstrado, de dar ensejo à ocorrência do evento previsto contrato.

Nos seguros de pessoas (vida e acidentes pessoais), os dados normalmente coletados pelas seguradoras não se referem única e exclusivamente à saúde do futuro segurado, mas também a seus hábitos, como por exemplo, se é fumante ou se prática esportes radicais, e também aqueles relativos a crédito, patrimônio e renda.

Os dados relativos a crédito, patrimônio e renda, que apesar de não estarem diretamente ligados ao objeto do seguro em questão, que é a vida ou a integridade física e psíquica do potencial segurado, são coletados e utilizados pelas seguradoras na verificação da compatibilidade de tais dados com o capital que se pretende segurar. Isto é, se os valores que o potencial segurado terá que pagar no decorrer dos anos a título de prêmio são compatíveis com sua renda e patrimônio e também se possui boas condições financeiras.

Tal análise tem o condão de identificar potenciais fraudes, como a prática de suicídios premeditados ou mesmo a automutilação.

Cabe mencionar que o atual Código Civil, entretanto, dificultou bastante o recebimento de indenizações decorrentes de suicídios premeditados, situação na qual a segurada contrata um seguro de vida de valor elevado e, pouco tempo depois, comete suicídio, deixando uma indenização para a família.

Existe a possibilidade, inclusive, de ser estabelecido um prazo de carência para o caso de morte do segurado, na forma do artigo 797 do Código Civil.

Corrobora desse entendimento o Superior Tribunal de Justiça – STJ, conforme se verifica abaixo:

> RECURSO ESPECIAL. AÇÃO DE COBRANÇA. SEGURO DE VIDA. SUICÍDIO DENTRO DO PRAZO DE DOIS ANOS DO INÍCIO DA VIGÊNCIA DO SEGURO. RECURSO ESPECIAL PROVIDO.
> 1. Durante os dois primeiros anos de vigência do contrato de seguro de vida, o suicídio é risco não coberto. Deve ser observado, porém, o direito do beneficiário ao ressarcimento do montante da reserva técnica já formada (Código Civil de 2002, art. 798 c/c art. 797, parágrafo único).
> 2. O art. 798 adotou critério objetivo temporal para determinar a cobertura relativa ao suicídio do segurado, afastando o critério subjetivo da premeditação. Após o período de carência de dois anos, portanto, a seguradora será obrigada a indenizar, mesmo diante da prova mais cabal de premeditação.
> 3. Recurso especial provido[62].

Cabe destacar, ainda, segundo orientação do Superior Tribunal de Justiça[63], que, na verdade, as seguradoras deveriam exigir que os potenciais segurados se submetessem a exames clínicos, laboratoriais e tantos outros, necessários à identificação de seu real estado de saúde:

> Ao rejeitar a alegação da recorrente que a doença que ocasionou óbito da segurada era preexistente à contratação do seguro, o Tribunal de origem asseverou que não foi exigido exame médico ou declaração a respeito do seu estado de saúde por ocasião da contratação do seguro, restando expressamente afastada a existência de má-fé com base nos seguintes fundamentos: "No mérito, aduz que o segurado tinha conhecimento da doença que culminou com sua morte, não tendo revelado sua situação quando da contratação do seguro. Observa-se que o apelante celebrou um contrato de seguro denominado Ouro Vida Produtor Rural, no qual pactuou seguro de vida, tratando-se na verdade de um contrato de adesão que é definido pela doutrina como sendo aquele em que as cláusulas são regradas unilateralmente por uma das partes. Trata-se de uma relação de consumo de modo que deve haver no caso em apreço a inversão do ônus da prova, nos termos do art. 6º, VIII, da Lei 8.070/90, a favor da apelada. Além disso, como é consabido, a boa-fé é presumida e a má-fé, ao contrário, deve ser provada. Sendo assim, a alegação da apelante de que o seguro contratado não seria devido em virtude de doença preexistente do segurado

[62] STJ - REsp: 1334005 GO 2012/0144622-7, Relator: Ministro PAULO DE TARSO SANSEVERINO, Data de Julgamento: 08/04/2015, S2 - SEGUNDA SEÇÃO, Data de Publicação: DJe 23/06/2015)
[63] (STJ - Ag: 1205814, Relator: Ministro RAUL ARAÚJO, Data de Publicação: DJ 25/10/2010

> não tem razão de subsistir, pois por ocasião da celebração do contrato não foi exigido do segurado exame médico ou declaração específica a respeito do seu estado de saúde, e não houve demonstração da sua má-fé ao preencher a proposta de contratação. Nesse sentido vê se a jurisprudência:“Contrato de Seguro. Se a seguradora aceita a proposta de adesão, mesmo quando segurado não fornece informações sobre o seu estado de saúde, assume os riscos do negócio. Não pode, por essa razão, ocorrendo o sinistro, recusar-se a indenizar.

Portanto, conclui-se que para a aplicação ideal dos princípios da finalidade e da informação à coleta e utilização desses dados, é necessário verificar a compatibilidade do dado coletado com o objeto do contrato e que há casos em que a coleta e a utilização de dados relativos a crédito, patrimônio e renda nos seguros de pessoas são legítimas.

Quanto à análise da coleta e utilização de dados relativos a hábitos, além da necessidade de observância dos princípios da finalidade e da informação, o dado coletado deve ser compatível com o objeto da relação jurídica entre o titular e o coletor do dado, no caso o objeto do contrato de seguro de pessoas.

Seguindo esse raciocínio, é razoável que a seguradora pergunte, por exemplo, ao potencial segurado, se ele é fumante, já que o fumo comprovadamente aumenta em muito a probabilidade de se desenvolver diversas doenças.

Da mesma forma nos parece razoável que a seguradora possa requerer informação relativa à prática de esportes radicais, que também aumenta a probabilidade de lesões e até de morte.

Quanto à prática de esportes, radicais ou não, o Código Civil, em seu artigo 799, considera nula a cláusula contratual que exime o segurador do pagamento da indenização caso a incapacidade ou morte seja dela decorrente.

Essa previsão, entretanto, não tem o condão de afastar o dever do potencial segurado de prestar tais informações, nem o direito da seguradora de usá-las para recusar um risco ou mesmo para majorar o valor do prêmio que irá cobrar em razão de o potencial segurado exercer tal prática e, portanto, apresentar mais riscos que a média das pessoas.

Outro exemplo de hábito que poderia interessar às seguradoras seria a condução de carros esportivos.

Entretanto, possuir um carro veloz não importa dizer que a pessoa o dirija perigosamente e, por isso, se exponha, maior risco, até porque existem restrições e limites de velocidade.

O objetivo da coleta e utilização desses dados é a melhor definição do risco a que está exposto o potencial segurado, e a delimitação das coberturas que estarão contempladas na apólice, uma vez que no seguro de pessoas, (diferente do que ocorre no seguro-saúde) não há um rol de coberturas predefinidas em lei, tendo plena aplicação o disposto nos artigos 757, 759 e 760 do Código Civil.

3.2 A proposta de regulamentação no Brasil sobre tratamento de dados e o contrato de seguro

Por fim, para concluir o presente estudo cumpre mencionar que à exemplo da legislação internacional que já regulamentou o tratamento de dados pessoais, o Brasil vem discutindo no âmbito do Congresso Nacional propostas legislativas para a regulamentação específica sobre o tema.

Há no âmbito do Congresso Nacional, o Projeto de Lei nº 4060, de 2012[64]; que *Dispõe sobre o tratamento de dados pessoais, e dá outras providência;* Projeto de Lei nº 5276 de 2016[65], que *Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural;* Projeto de Lei do Senado nº 330, de 2013[66], que *dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências*; Projeto de Lei do Senado nº 131 de 2014[67] , que *dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros* e Projeto de Lei do Senado nº 181 de 2014[68], que *estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais*.

---

[64] Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066&ord=1 Acesso 18 mai. 2017.
[65]Disponível em:< http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378> Acesso em 18 mai. 2017.
[66] Disponível em:< http://www25.senado.leg.br/web/atividade/materias/-/materia/113947> Acesso em 18 mai. 2017.
[67] Disponível em:http://www25.senado.leg.br/web/atividade/materias/-/materia/117736 Acesso em 18 mai. 2017.
[68] Disponível em:< http://www25.senado.leg.br/web/atividade/materias/-/materia/116969> Aceso em 18 mai. 2017.

Dentre as propostas de regulamentação, destacamos o PL nº 5276/16, tendo em vista que foi oriundo um anteprojeto de lei do Ministério Público Federal, objeto de consulta pública.

O PL nº 5276/16 estabelece que a disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e:

> **(i)** A autodeterminação informativa;
> **(ii)** Liberdade de expressão, de comunicação e de opinião;
> **(iii)** A inviolabilidade da intimidade, da vida privada, da honra e da imagem;
> **(iv)** O desenvolvimento econômico e tecnológico e
> **(v)** A livre iniciativa, a livre concorrência e a defesa do consumidor[69].

Ao disciplinar a proteção de dados pessoais com respeito aos itens acima, a proposta assegura que haverá um equilíbrio e ponderação entre esses aspetos, o que é de vital importância para a sustentabilidade do setor de seguros.

Além disso, o PL determina, entre outros, os seguintes conceitos:

> **Dado pessoal:** dado relativo à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;
> **Tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> **Dados sensíveis**: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos.
> **Dados anonimizados** – dados relativos a um titular que não possa ser identificado;
> **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada[70].

Também prevê o PL como princípios das atividades de tratamento de dados pessoais, além da boa-fé, os seguintes princípios:

---

[69] Art. 2º do PL nº 5276/16. Op Cit
[70] Disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 Acesso em 18 mai. 2017.

> I – finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;
> II – adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;
> III – necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV – livre acesso: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;
> V – qualidade dos dados: pelo qual devem ser garantias aos titulares a exatidão, a clareza, relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;[71]
> VI – transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;
> VII – segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII – prevenção: pelo qual devem ser adotadas medidas para prevenir a ocorrência de dados em virtude do tratamento de dados pessoais; e
> IX – não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios.[72]

Ademais, o PL prevê que o tratamento de dados pessoais somente poderá ser realizado nas hipóteses de[73]:

> I -Fornecimento pelo titular de consentimento livre, informado e inequívoco;
> II - Para cumprimento de uma obrigação legal pelo responsável e pela administração pública;
> III - Para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;
> IV - Para a realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais, quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;
> V - Para o exercício regular de direitos em processo judicial ou administrativo; para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VI - Quando necessário para atender aos interesses legítimos do responsável ou de terceiro exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titula que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

Cabe mencionar que os termos do projeto de lei estão de acordo com os princípios ditos anteriormente, quais sejam da publicidade (ou da transparência), da exatidão da finalidade, do

[71] PL 5276/16. Op. cit p. 3.
[72]Disponível em:< http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378> Acesso em 18 mai. 2017.p. 4
[73] PL 5276/16. Op. cit p.5

livre acesso e da segurança física e lógica, que são base para as normas internacionais sobre a proteção de dados pessoais.

O Projeto de Lei dispõe que o titular deverá ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva sobre, tendo ciência inclusive, entre outros, a:

> (i) A finalidade específica do tratamento;
> (ii) A forma e duração do tratamento;
> (iii) A identificação do responsável;
> (iv) Informações de contrato do responsável;
> (v) Sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados e o âmbito de sua difusão;
> (vi) Responsabilidades dos agentes que realizarão o tratamento; e
> (vii) Direitos do titular, com menção explícita à possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado e denunciar ao órgão competente a eventual descumprimento.[74]

Há a previsão no projeto de que o consumidor não será obrigado a fornecer o consentimento para a contratação do serviço, na hipótese em que o consentimento requerido, mediante o fornecimento de informações sobre as consequências da negativa.

Quando o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço para o exercício de direito, o titular deverá ser informado com destaque sobre tal fato e por quais poderá exercer controle sobre o tratamento de seus dados.

Além disso, este será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou não tenham sido apresentadas previamente de forma clara, adequada e ostensiva.

Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado periodicamente sobre as principais características do tratamento, nos termos definidos pelo órgão competente.

Destaca-se que o consentimento deverá ser livre, informado e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique.

---

[74] PL 5276/16. Op. cit p.5

Caso o consentimento seja fornecido por escrito, este deverá ser fornecido em cláusula destacada das demais cláusulas contratuais.

Será vedado o tratamento de dados pessoais quando o consentimento tenha sido obtido mediante erro, dolo, coação, estado de perigo ou simulação.

O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais e poderá ser revogado a qualquer momento, mediante manifestação expressa do titular. Em caso de alteração de informação deverá obter-se novo consentimento do titular, após destaque de forma específica o teor das alterações.

O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais quando necessário e baseado em uma situação concreta, respeitados os direitos e liberdades fundamentais do titular, que deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados.

O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse, devendo fornecer aos titular mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.

Quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.

O PL nº 5276/16 também prevê que sobre os dados anonimizados serão considerados dados pessoais, quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido para a identificação do indivíduo.

Quanto ao tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse.

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses de:

(i) Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
(ii) Fim do período de tratamento;
(iii) Comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento;
(iv) Determinação do órgão competente, quando houver violação da legislação em vigor a respeito[75].

Após o término do tratamento de dados pessoais, estes serão eliminados podendo ser autorizada a conservação para o cumprimento de obrigação legal do responsável, pesquisa histórica, científica ou estatística, garantida, quando possível, a anonimização dos dados pessoais; ou transferência a terceiros, desde que respeitados os requisitos de tratamento de dados.

Além disso, o PL nº 5276/16 veda o tratamento de dados pessoais sensíveis, exceto, quando na hipótese de com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no seu tratamento.

O referido PL também assegura que toda pessoa natural terá a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade.

Dessa forma, o titular dos dados pessoais tem direito a obter, em relação aos seus dados:

(i) Confirmação da existência de tratamento;
(ii) Acesso aos dados;
(iii) Correção de dados incompletos, inexatos ou desatualizados;
(iv) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos;
(v) Portabilidade, mediante requisição, de seus dados pessoais a outro fornecedor de serviço ou produto;
(vi) Limitação, a qualquer momento, de dados pessoais cujo tratamento o titular tenha consentido[76].

[75]Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378> acesso m 18 mai. 2017, p. 8.

Destarte, o PL determina que a transferência internacional de dados pessoas somente é permitida nos seguintes casos:

> (i) Para países que proporcionem nível de proteção de dados pessoais ao menos equiparável;
> (ii) Quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e investigação, de acordo com os instrumentos de direito internacional;
> (iii) Quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro
> (iv) Quando o órgão competente autorizar a transferência;
> (v) Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> (vi) Quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público;
> (vii) Quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos[77]

Destaca-se que, os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou do conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

Mister se faz necessário adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

Somente o órgão competente poderá dispor sobre padrões técnicos e organizacionais, levando-se em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis. As medidas de segurança deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução, como forma de preservar os dados dos indivíduos.

---

[76] Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378> acesso m 18 mai. 2017, p. 8.
[77]Disponível em: < http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016 > Acesso em 18 mai. 2017

Com a globalização e o avanço tecnológico da informação é fundamental a proteção da informação e dados pessoais a fim de resguardar a intimidade, privacidade e individualidade das pessoas e liberdades individuais, assegurando aos indivíduos o efetivo conhecimento e controle sobre seus próprios dados, sem causar impacto na economia, respeitando-se os princípios das atividades de tratamento de dados pessoais, bem como o dever de boa-fé como um dos princípios basilares do nosso ordenamento jurídico.

Isto posto, a aprovação do projeto terá grande importância no ordenamento jurídico brasileiro, e em especial grande impacto para as sociedades seguradoras que deverão se adaptar a nova legislação, criando meios para a proteção de pessoas e patrimônio, gerando receitas, tributos e auxiliando no desenvolvimento econômico do país, especialmente no setor de seguros.

4. CONCLUSÃO

O avanço tecnológico impactou a sociedade, tornando o direito à privacidade mais complexo.

Assim sendo, a buscou-se estabelecer mecanismos para a proteção da ameaça à privada na forma de vigilância física, vigilância psicológica e controle de dados.

O ordenamento jurídico internacional avançou nesse sentido e criou regulamentação específica para a proteção do tratamento de dados pessoais.

Os dois principais modelos de regulamentação sobre o assunto são o modelo Europeu e o modelo dos Estados Unidos, sendo o modelo Europeu mais difundido.

Cabe esclarecer que até a chegar à forma atual a regulamentação de dados internacional passou por diversas transformações.

Atualmente, a proteção de dados pessoais é pautada nos princípios da autodeterminação, da publicidade (ou da transparência), da exatidão, da finalidade, do livre acesso e da segurança física e lógica.

Desses princípios se extrai que para o tratamento de dados pessoais, que o indivíduo deve ser consentir, e para o efetivo consentimento ser informado da forma como será utilizado seu dado, do motivo para utilização, pelo tempo de uso e ser assegurado quanto a segurança de seus dados.

No caso do Brasil, ainda não há uma regulamentação específica em vigor para o tratamento de dados pessoais, sendo vista sob a ótica das garantias estabelecidas quanto ao direito à privacidade prevista na Constituição Federal, Código Civil, Código de Defesa do Consumidos, Lei do Marco Civil.

A ausência de regulamentação deixa os indivíduos a mercê de diversas práticas de violação do uso de dados.

Sobre o contrato de seguro, verifica-se que é baseado no princípio do mutualismo, em que os segurados cooperam para um fundo comum, que é administrado pela seguradora.

Como administradora do fundo comum, decorrem da responsabilidade da seguradora a melhor precificação e utilização das quantias do fundo.

Dentro desse aspecto, as informações são essenciais para a precificação do cálculo atuarial e melhor administração do fundo.

Considerando essas informações, o estudo em apreço analisou o setor de seguros à luz dos princípios da proteção de dados pessoais, de forma que seja garantido ao indivíduo a privacidade e a autodeterminação da sua vontade, sem que seja inviabilizada a operação do setor de seguros.

Para tal análise, foi utilizado o Projeto de Lei nº 5276/16, uma das propostas que se encontra no Congresso Nacional para a regulamentação específica do tratamento de dados pessoais.

Neste sentido, foi avaliada na análise que a interpretação do consentimento do segurado deve ser associada ao seu efetivo direito a informação sobre o contrato de seguros e seus dados.

Dentro dessa análise, foi visto que o PL nº 5276/16 atenderá em grande parte a efetiva proteção do consumidor e setor de seguro, já que estabelece o equilíbrio entre a privacidade e a livre iniciativa.

Outrossim, foi visto que difícil é, portanto, estabelecer o limite para a coleta de tais dados pelas seguradoras, se ela é legitima ou não, e consequentemente, se tais dados fazem parte apenas do estilo de vida de cada pessoa e, portanto, devem ser preservados, como esfera de sua privacidade.

Isto posto, não se justificaria a coleta de informações de saúde dos potenciais segurados, mas somente aquelas relativas a alguns hábitos e a lesões preexistentes, estas últimas com o

fim de verificar eventual incapacidade do potencial segurado, como decorrência de acidente sofrido em data anterior à contratação do seguro.

A verificação da legitimidade da coleta desses dados deverá alicerçar-se, mais uma vez, nos princípios da informação e da finalidade, e na compatibilidade do dado com o objeto do contrato (princípio da proporcionalidade).

Assim sendo, conclui-se que a aprovação do projeto de Lei nº 5276/16 será um grande avanço para o Brasil, no sentido de maior proteção dos dados pessoais dos indivíduos, visto que não inviabilizará o tratamento de dados pessoais no setor de seguros.

REFERÊNCIAS BIBLIOGRÁFICAS

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

MARTINS. Guilherme Magalhães**. Direito Privado e Internet.** São Paulo: Atlas, 2014.

RIBEIRO, Amadeu Carvalhães. **Direito de Seguros: resseguro, seguro direto e distribuição de serviços** – São Paulo: Atlas, 2006

MARTINS. Guilherme Magalhães **. Responsabilidade Civil por acidente de consumo na internet**. São Paulo. Revista dos Tribunais., 2008, p. 238-239.

MIRAGEM, Bruno. **Curso de direito do consumidor** – 6. Ed. rev., atual. e ampl. – São Paulo: Editora Revista dos Tribunais, 2016.

NEGREIROS, Teresa. **Fundamentos para uma interpretação constitucional do princípio da boa-fé**. Rio de Janeiro, Renovar, 2002

BARROSO, Luís Roberto. **Viagem redonda: habeas data, direitos constitucionais e provas ilícitas**. In: WAMBIER, Teresa Arruda Alvim (Coord.). Habeas data. São Paulo: RT, 1998.

GONÇALVES, Maria Eduarda, ***Direito da informação***. Coimbra: Almedina, 1995.

BENNETT, Colin. **Regulating privacy. Data protection and public policy in Europe and UnitedStates**. Itahaca: Cornell University Press, 1992.

CASTELLS, Manuel. **A sociedade em rede (A era da informação, economia, sociedade e cultura)**. São Paulo: Paz e Terra, 1999. v. 1.

CARVALHO, Ana Paula Gambogi. **O consumidor e o direito à autodeterminação informacional**. Revista de Direito do Consumidor, n. 46, p. 77-119, abr./jun. 2003.

CARVALHO, Luis Gustavo Grandinetti de. **Direito de Informação e Liberdade de Expressão**. Rio de Janeiro: Renovar, 1999.

CATALA, Pierre. **Ebauche d' une théorie juridique de l'information. Informatica e Dirito**, ano 9, p. 20, janv./avril 1983.

DALLARI, Dalmo de Abreu. **O habeas data no sistema jurídico brasileiro**. Revista de la Faculdade de derecho de La Pontifícia Universidade Católica del Peru, n. 51, p. 100, 1997.

FERRAZ JÚNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Revista da Faculdade de Direito da Universidade de São Paulo. 1993. v. 88.

SAMPAIO, José Adércio Leite Sampaio**. Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1997.

LIMBERGER, Têmis. O direito à intimidade na era da informática. Porto Alegre: Livraria do Advogado, 2007.

Novas tendências do direito do consumidor: Rede Alemanha-Brasil de pesquisas em direito do consumidor / Claudia Lima Marques, Beate Gsell, (organizadoras) – São Paulo: Editora Revista dos Tribunais, 2015.

RODOTÀ, Stefano. Elaboratori elettronici e controllo sociale. Bologna: II Mulino, 1973. Repentino di fine secolo. Bari: Laterza, 1999.

RODOTÀ, STEFANO. Tecnologie e diritti. Bologna: Mulino, 1995

SHILS. EDWARD. **Privacy.** ***Its constitution and vicissitudes***. Law and contemporary problem, 2/1996.

WACKS, Raymond. **Personal information**. Oxford: Clarendon Pressa, 1989

GARFINKEL, **Simson. Database nation**. Sebastopol: O'Reillly, 2000.

JEWKES, Yvonne (Ed.). The media studies reader. London: Arnold, 1998.

RICCIUTO, **Vicenzo. La disciplina Del trattamento dei dati personali**. Giappechelli, 1997.

MAYER – SCONBERGER, Viktor. "General development of data protection in Europe", in Technology and privacy: Thechnology and privacy: The new landscape. AGRE, Phillip;

ROTENBERG,Marc, (orgs). Cambridge: MIT Press, 1997, pp. 219-242 apud, DONEDA, 2006. p. 352.

WESTIN, Alan, Privacy and freedom, new York: Athencum, Signet, 1972, pp. 259-260, apud DONEDA, 2006, p. 161

ROTENBERG, Marc (Org.). **Technology and privacy: The new landscape**. Cambridge: MIT Press, 1997. MILLER, Arthur. Assault on privacy. Ann Arbor: University of Michigan, 1971.

PERLINGIERI, Pietro. **L' informazione come bene giuridico**. In: Rassegna di diritto civile. 2/90, p. 329.

PINÃR MAÑAS, José Luis. El derecho fundamental a la protección de dados personales (LOPD). In: (Dir.). **Protección de datos de carácter personal en Iberoamérica**.

VALENCIA: Tirant Lo Blanch, 2005. PUCCINELLI, Oscar. **El habeas data em Indoiberoamérica**. Bogotá: Temis, 1999.

EUA. **Records, computers and the rights of citizens**. Reporto of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973.

BRASIL, Constituição Federal, art. 5º, incisos X e XI. Disponível em < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm > Acesso em 26 de maio de 2017.

BRASIL, Código Civil, art. 21. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm> Acesso em 27 de maio de 2017.

V Jornada do Direito Civil / Organização Ministro Ruy Rosado de Aguiar Jr. – Brasília: CJF, 2011. Disponível em: http://www.cjf.jus.br/enunciados/enunciado/208 . Acesso em 08 mai. 2017.

BRASIL, Código de Defesa do Consumidor, art. 43. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em 08 mai.2017.

BRASIL, Código Penal, artigos 150 a 154. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 14 mai. 2017.

Resolução CNSP n 294/13. Disponível em: http://www2.susep.gov.br/bibliotecaweb/docOriginal.aspx?tipo=1&codigo=31432 Acesso em 18 mai. 2017.

Projeto de Lei 5276/16. Disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 Acesso em 18 mai. 2017.

BRASIL. STJ, Recurso Especial nº 22.337/RS, Relator Ministro Ruy Rosado de Aguiar. Disponível em: https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=3&formato=PDF . Acesso em 18 mai. 2017.